(19)日本国特許庁（ＪＰ)　(12) 公開特許公報（Ａ)　(11)特許出願公開番号
特開平7－297818
(43)公開日　平成７年(1995)11月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ 9/00				
9/10				
9/12				
Ｇ０６Ｆ 15/00	３３０	Ｇ 7459－5Ｌ		
			Ｈ０４Ｌ 9/00	Ｚ

審査請求　未請求　請求項の数２　ＯＬ　(全 12 頁)　最終頁に続く

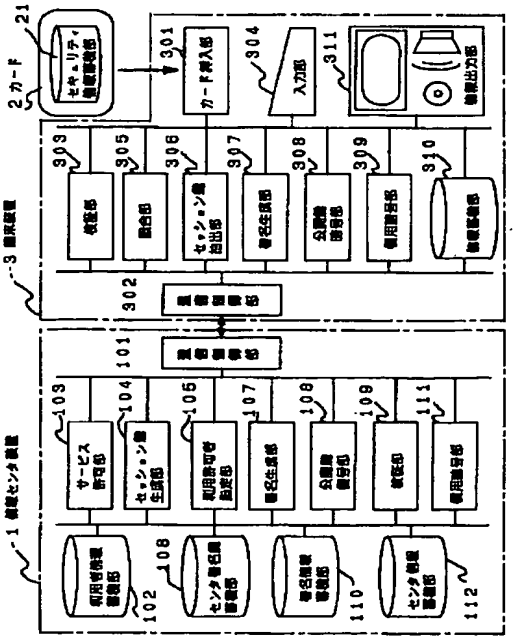
(21)出願番号　特願平6－86837

(22)出願日　平成６年(1994)４月25日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　神田　雅透
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　吉田　精孝

(54)【発明の名称】　ディジタル情報通信システム及びその方法

(57)【要約】
【目的】　通信利用により受信・購入した有料のディジタル情報について、複数人で構成される特定の正規利用者グループにとってはバックアップ等のコピーの自由や受信端末以外の端末での利用を可能にし、また著作権者や情報提供者にとっては正規の利用者グループ以外の不正利用を防止し、著作権が保護されるディジタル情報通信システム及びその方法を提供する。
【構成】　各カードごとに異なる利用者識別番号及びグループに一つだけ共通に設定されるグループ秘密鍵等を蓄積したセキュリティ情報蓄積部２１を有するカード２を設け、カード２と端末装置３とを接続し、カード２に蓄積されている利用者識別番号を端末装置３から情報センタ装置１に送信して情報を要求し、受信した情報本体をグループ秘密鍵を用いて暗号化して端末装置３内に蓄積し、この情報本体を利用する際には、グループ秘密鍵によって情報本体を復号する。



【特許請求の範囲】

【請求項１】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、端末装置に蓄積した後、復号してから利用するディジタル情報通信システムにおいて、

１グループに複数枚発行されるカードを設け、該カードには、各カードごとに異なる利用者識別番号と利用者署名鍵及びグループに一つだけ共通に設定されるグループコードとグループ秘密鍵、さらにシステム共通のセンタ検証鍵を蓄積するセキュリティ情報蓄積手段を有し、

前記情報センタ装置は、前記端末装置との間での通信を制御する通信制御手段と、

カードごとに対応するグループコードと利用者識別番号とセンタ登録パスワードと利用者検証鍵及び提供を受けることができるサービスを規定した提供サービス情報を蓄積する利用者情報蓄積手段と、

前記提供サービス情報に基づいて情報の提供の可否を判定するサービス許可手段と、

ディジタル情報本体を暗号化するセッション鍵を生成するセッション鍵生成手段と、

受信・蓄積した情報を利用できる利用者を指定する利用許可者指定手段と、

センタの署名鍵を蓄積するセンタ署名鍵蓄積手段と、

前記セッション鍵に対して前記センタ署名鍵によってディジタル署名を生成する署名生成手段と、

公開鍵暗号方式により前記端末装置から受信した暗号化署名情報の復号化を行なう公開鍵復号手段と、

端末装置からのディジタル情報を検証する検証手段と、

端末装置からの前記ディジタル情報を蓄積する署名情報蓄積手段と、

慣用暗号方式により前記セッション鍵を用いて前記ディジタル情報の暗号化を行なう慣用暗号手段と、

ディジタル情報本体を蓄積するセンタ情報蓄積手段とを備え、

前記端末装置は、前記カードのセキュリティ情報蓄積手段内の情報を読み取るカードインタフェース手段と、

前記情報センタ装置との間での通信を制御する通信制御手段と、

前記情報センタ装置から受信したディジタル署名情報を検証する検証手段と、

パスワードの入力やサービスを利用できる利用者を指定する情報を入力するための入力手段と、

利用者の照合を行なう照合手段と、

ディジタル情報本体を暗号化しているセッション鍵を抽出するセッション鍵抽出手段と、

前記セッション鍵に対して前記カードに蓄積された利用者署名鍵を用いてディジタル署名を生成する署名生成手段と、

公開鍵暗号方式により、前記署名生成手段により得られた前記署名情報を前記センタ検証鍵によって暗号化を行なう公開鍵暗号手段と、

慣用暗号方式により暗号化／復号を行なう慣用暗号手段と、

受信情報を蓄積する情報蓄積手段と、

受信情報を読み出して利用できるメディア情報に変換出力する情報出力手段とを備えていることを特徴とするディジタル情報通信システム。

【請求項２】　音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、端末装置に蓄積した後、復号してから利用するディジタル情報通信方法であって、

各カードごとに異なる利用者識別番号と利用者署名鍵及びグループに一つだけ共通に設定されるグループコードとグループ秘密鍵、さらにシステム共通のセンタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカードを設けると共に、該カードを１グループに複数枚発行し、

端末装置では、前記複数枚のグループカードのうちの１枚のカードから該カードの蓄積データを抽出すると共に、情報センタ装置に接続した後、受信・蓄積する情報を利用できるグループ内の全てまたは一部のメンバーの利用者識別番号からなる利用者リストを入力手段から入力し、前記カードのセキュリティ情報蓄積手段より抽出したグループコードと利用者識別番号と共に前記利用者リストを前記情報センタ装置に送信してディジタル情報の送信を要求し、

該要求を受けた情報センタ装置では、利用者情報蓄積手段より前記受信した利用者識別番号に対応するセンタ登録パスワード、利用者検証鍵、及び提供サービス情報を抽出し、次いで、前記提供サービス情報を基に前記送信要求されたディジタル情報の提供の可否を判定し、否の場合には回線を切断し、可の場合には疑似セッション鍵と照合セッション鍵の２種類のセッション鍵を生成し、

前記疑似セッション鍵と照合セッション鍵から第１の秘密関数によりセッション鍵を生成した後に、前記利用者リストに指定される利用者識別番号、前記利用者情報蓄積手段より前記グループコード及び前記指定される利用者識別番号に基づいて抽出されたセンタ登録パスワード、並びに前記照合セッション鍵から第２の秘密関数により照合用リストを作成し、前記受信した利用者識別番号並びに抽出したセンタ登録パスワード、前記疑似セッション鍵、前記照合セッション鍵及び前記照合用リストを第３の秘密関数で変換し、該変換結果をセンタ署名鍵蓄積手段より抽出したセンタ署名鍵で署名したセンタ署名情報を前記端末装置に送信し、

該情報を受信した端末装置では、前記センタ署名情報から前記カードのセキュリティ情報蓄積手段より抽出したセンタ検証鍵を用いて利用者識別番号を抽出し、前記送信した利用者識別番号との検証を行ない、不一致の場合

においては回線を切断し、一致の場合には利用者に対してパスワードの入力を要求し、前記入力されたパスワード及び前記センタ署名情報から第４の秘密関数により変換して疑似セッション鍵、照合セッション鍵及び照合用リストを抽出し、前記疑似セッション鍵と前記照合セッション鍵から第１の秘密関数によりセッション鍵を構成した後、前記利用者識別番号、前記パスワード及び前記照合セッション鍵から第２の秘密関数により利用者照合データを作成し、該利用者照合データと前記照合用リストとの比較照合を行ない、該比較結果が不一致の場合には回線を切断し、一致の場合には前記構成したセッション鍵から前記カードのセキュリティ情報蓄積手段より抽出した利用者署名鍵を用いて利用者署名情報を生成した後、前記センタ検証鍵により前記利用者署名情報を暗号化して前記情報センタ装置に送信し、

前記利用者署名情報を受信した情報センタでは、前記センタ署名鍵を用いて前記暗号化された利用者署名情報を復号し、前記利用者署名情報を署名情報蓄積手段に蓄積した後、前記利用者署名情報から前記利用者情報蓄積手段に蓄積されている利用者検証鍵を用いてセッション鍵を抽出し、該抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には回線を切断し、一致の場合には前記送信要求されたディジタル情報をセンタ情報蓄積手段から取り出し、前記ディジタル情報を前記セッション鍵で暗号化したうえで前記端末装置に送信し、

前記暗号化ディジタル情報を受信した端末装置では、前記セッション鍵抽出手段で抽出した疑似セッション鍵、照合セッション鍵及び照合用リストを前記カードのセキュリティ情報蓄積手段より抽出したグループ秘密鍵で暗号化し、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積する情報配送過程と、

前記端末装置において、前記情報配送過程で利用したカードを含む複数枚のグループカードのうちの１枚のカードから該カードの蓄積データを抽出すると共に、利用者に対してパスワードの入力を要求し、前記情報蓄積手段内の利用したい情報に対応する前記暗号化された照合セッション鍵及び照合用リストを前記グループ秘密鍵で復号し、前記入力されたパスワード、前記復号された照合セッション鍵及び前記カードに蓄積されている利用者蓄積番号から第２の秘密関数により利用者照合データを作成し、該利用者照合データと前記復号された照合用リストとの比較照合を行ない、該比較照合結果が不一致の場合には情報の利用を禁止し、一致の場合には前記暗号化された疑似セッション鍵を前記グループ秘密鍵で復号し、前記復号された疑似セッション鍵と前記照合セッション鍵から第１の秘密関数によりセッション鍵を再構成した後、前記セッション鍵により暗号化されたディジタル情報本体を復号して情報出力手段から出力する情報利用過程とを有することを特徴とするディジタル情報通信方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信回線を利用して情報配送センタから音楽、映像、プログラム等の暗号化されたディジタル著作物情報を受信端末に受信・蓄積した後、実際の利用時において正規の個別のカードを所有し、かつパスワードを知っている複数人の利用者グループに限り、受信端末に接続することにより端末の制限を受けずに利用でき、また情報提供者にとっては著作権が保護されることを考慮したディジタル情報通信システム及びその方法に関するものである。

【０００２】

【従来の技術】従来、音声、動画、静止画などのディジタル情報圧縮技術、及び高速ディジタル通信技術の発達により、音楽、映像、ソフトウェア等の著作物をディジタル情報に変換、圧縮符号化して通信回線を利用して送信することが可能となってきた。特に、ソフトウェアについてはすでにパソコン通信等を利用した配送サービスが実施されている例があり、このように通信回線を利用して情報配送センタから希望のディジタル情報を送信してもらう、いわゆる「オンデマンドサービス」では従来の流通経路が簡略化されるため、経済的でかつ迅速に情報を全国配送できる利点がある。

【０００３】

【発明が解決しようとする課題】しかしながら、通信利用により受信・蓄積したディジタル情報は一般に利用制限などの対策が取りにくく、ディジタル情報が有料の著作物である場合にはその有料ディジタル情報を購入して受信・蓄積した正規の利用者だけでなく、他の人の不正利用を招いたり、不正コピーが横行するなどして著作権が侵害され、著作権者や情報提供業者の利益を損ねる問題があった。

【０００４】一方、不正利用や不正コピーを防止するため、コピー自体を禁止する対策が取られる場合があるがこの場合は正規の利用者にとってバックアップができない、情報を受信した端末装置でなければ利用できないなどの不都合が生じる。このように、利用制限や制約を大きくすると利用人数が一人に限定されることになり、グループ契約（家族／企業内セクション等）などのサービスを実現することが困難である。

【０００５】本発明の目的は上記の問題点に鑑み、通信利用により受信・購入した有料のディジタル情報について、複数人で構成される特定の正規利用者グループにとってはバックアップなどのコピーの自由や受信端末以外の端末での利用を可能にし、また著作権者や情報提供者にとっては正規の利用者グループ以外の不正利用を防止し、著作権が保護されるディジタル情報通信システム及びその方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明は上記の目的を達成するために、請求項１では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、端末装置に蓄積した後、復号してから利用するディジタル情報通信システムにおいて、１グループに複数枚発行されるカードを設け、該カードには、各カードごとに異なる利用者識別番号と利用者署名鍵及びグループに一つだけ共通に設定されるグループコードとグループ秘密鍵、さらにシステム共通のセンタ検証鍵を蓄積するセキュリティ情報蓄積手段を有し、前記情報センタ装置は、前記端末装置との間での通信を制御する通信制御手段と、カードごとに対応するグループコードと利用者識別番号とセンタ登録パスワードと利用者検証鍵及び提供を受けることができるサービスを規定した提供サービス情報を蓄積する利用者情報蓄積手段と、前記提供サービス情報に基づいて情報の提供の可否を判定するサービス許可手段と、ディジタル情報本体を暗号化するセッション鍵を生成するセッション鍵生成手段と、受信・蓄積した情報を利用できる利用者を指定する利用許可者指定手段と、センタの署名鍵を蓄積するセンタ署名鍵蓄積手段と、前記セッション鍵に対して前記センタ署名鍵によってディジタル署名を生成する署名生成手段と、公開鍵暗号方式により前記端末装置から受信した暗号化署名情報の復号化を行なう公開鍵復号手段と、端末装置からのディジタル情報を検証する検証手段と、端末装置からの前記ディジタル情報を蓄積する署名情報蓄積手段と、慣用暗号方式により前記セッション鍵を用いて前記ディジタル情報の暗号化を行なう慣用暗号手段と、ディジタル情報本体を蓄積するセンタ情報蓄積手段とを備え、前記端末装置は、前記カードのセキュリティ情報蓄積手段内の情報を読み取るカードインタフェース手段と、前記情報センタ装置との間での通信を制御する通信制御手段と、前記情報センタ装置から受信したディジタル署名情報を検証する検証手段と、パスワードの入力やサービスを利用できる利用者を指定する情報を入力するための入力手段と、利用者の照合を行なう照合手段と、ディジタル情報本体を暗号化しているセッション鍵を抽出するセッション鍵抽出手段と、前記セッション鍵に対して前記カードに蓄積された利用者署名鍵を用いてディジタル署名を生成する署名生成手段と、公開鍵暗号方式により、前記署名生成手段により得られた前記署名情報を前記センタ検証鍵によって暗号化を行なう公開鍵暗号手段と、慣用暗号方式により暗号化／復号を行なう慣用暗号手段と、受信情報を蓄積する情報蓄積手段と、受信情報を読み出して利用できるメディア情報に変換出力する情報出力手段とを備えているディジタル情報通信システムを提案する。

【０００７】また、請求項２では、音声、音楽、映像、文字の少なくとも一つからなる暗号化されたディジタル情報を情報センタ装置から通信回線を経由して受信し、端末装置に蓄積した後、復号してから利用するディジタル情報通信方法であって、各カードごとに異なる利用者識別番号と利用者署名鍵及びグループに一つだけ共通に設定されるグループコードとグループ秘密鍵、さらにシステム共通のセンタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカードを設けると共に、該カードを１グループに複数枚発行し、端末装置では、前記複数枚のグループカードのうちの１枚のカードから該カードの蓄積データを抽出すると共に、情報センタ装置に接続した後、受信・蓄積する情報を利用できるグループ内の全てまたは一部のメンバーの利用者識別番号からなる利用者リストを入力手段から入力し、前記カードのセキュリティ情報蓄積手段より抽出したグループコードと利用者識別番号と共に前記利用者リストを前記情報センタ装置に送信してディジタル情報の送信を要求し、該要求を受けた情報センタ装置では、利用者情報蓄積手段より前記受信した利用者識別番号に対応するセンタ登録パスワード、利用者検証鍵、及び提供サービス情報を抽出し、次いで、前記提供サービス情報を基に前記送信要求されたディジタル情報の提供の可否を判定し、否の場合には回線を切断し、可の場合には疑似セッション鍵と照合セッション鍵の２種類のセッション鍵を生成し、前記疑似セッション鍵と照合セッション鍵から第１の秘密関数によりセッション鍵を生成した後に、前記利用者リストに指定される利用者識別番号、前記利用者情報蓄積手段より前記グループコード及び前記指定される利用者識別番号に基づいて抽出されたセンタ登録パスワード、並びに前記照合セッション鍵から第２の秘密関数により照合用リストを作成し、前記受信した利用者識別番号並びに抽出したセンタ登録パスワード、前記疑似セッション鍵、前記照合セッション鍵及び前記照合用リストを第３の秘密関数で変換し、該変換結果をセンタ署名鍵蓄積手段より抽出したセンタ署名鍵で署名したセンタ署名情報を前記端末装置に送信し、該情報を受信した端末装置では、前記センタ署名情報から前記カードのセキュリティ情報蓄積手段より抽出したセンタ検証鍵を用いて利用者識別番号を抽出し、前記送信した利用者識別番号との検証を行ない、不一致の場合においては回線を切断し、一致の場合には利用者に対してパスワードの入力を要求し、前記入力されたパスワード及び前記センタ署名情報から第４の秘密関数により変換して疑似セッション鍵、照合セッション鍵及び照合用リストを抽出し、前記疑似セッション鍵と前記照合セッション鍵から第１の秘密関数によりセッション鍵を構成した後、前記利用者識別番号、前記パスワード及び前記照合セッション鍵から第２の秘密関数により利用者照合データを作成し、該利用者照合データと前記照合用リストとの比較照合を行ない、該比較結果が不一致の場合には回線を切断し、一致の場合には前記構成したセッション鍵から前記カードのセキュリティ情報蓄積手段より抽出した利用者署名鍵を用いて利用者

署名情報を生成した後、前記センタ検証鍵により前記利用者署名情報を暗号化して前記情報センタ装置に送信し、前記利用者署名情報を受信した情報センタでは、前記センタ署名鍵を用いて前記暗号化された利用者署名情報を復号し、前記利用者署名情報を署名情報蓄積手段に蓄積した後、前記利用者署名情報から前記利用者情報蓄積手段に蓄積されている利用者検証鍵を用いてセッション鍵を抽出し、該抽出したセッション鍵と前記生成したセッション鍵とを照合し、該照合結果が不一致の場合には回線を切断し、一致の場合には前記送信要求されたディジタル情報をセンタ情報蓄積手段から取り出し、前記ディジタル情報を前記セッション鍵で暗号化したうえで前記端末装置に送信し、前記暗号化ディジタル情報を受信した端末装置では、前記セッション鍵抽出手段で抽出した疑似セッション鍵、照合セッション鍵及び照合用リストを前記カードのセキュリティ情報蓄積手段より抽出したグループ秘密鍵で暗号化し、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積する情報配送過程と、前記端末装置において、前記情報配送過程で利用したカードを含む複数枚のグループカードのうちの１枚のカードから該カードの蓄積データを抽出すると共に、利用者に対してパスワードの入力を要求し、前記情報蓄積手段内の利用したい情報に対応する前記暗号化された照合セッション鍵及び照合用リストを前記グループ秘密鍵で復号し、前記入力されたパスワード、前記復号された照合セッション鍵及び前記カードに蓄積されている利用者蓄積番号から第２の秘密関数により利用者照合データを作成し、該利用者照合データと前記復号された照合用リストとの比較照合を行ない、該比較照合結果が不一致の場合には情報の利用を禁止し、一致の場合には前記暗号化された疑似セッション鍵を前記グループ秘密鍵で復号し、前記復号された疑似セッション鍵と前記照合セッション鍵から第１の秘密関数によりセッション鍵を再構成した後、前記セッション鍵により暗号化されたディジタル情報本体を復号して情報出力手段から出力する情報利用過程とを有するディジタル情報通信方法を提案する。

【０００８】

【作用】本発明の請求項１記載のディジタル情報通信システムによれば、利用者が、情報センタ装置内の情報を端末装置に受信・蓄積する際には、利用者の所有するカードが端末装置のカードインタフェース手段に接続され、通信制御手段を介して端末装置と情報センタ装置が接続される。この後、入力手段を介してパスワード及び利用者を指定する情報が入力され、該情報と前記カードのセキュリティ情報蓄積手段から抽出されたグループコードと利用者識別番号とが情報センタ装置に送信され、ディジタル情報の送信要求が行われる。また、カードのセキュリティ情報蓄積手段に蓄積された情報内容は物理的に保護されている。

【０００９】送信要求を受けた情報センタ装置では、利用者情報蓄積手段より、端末装置から受信した利用者識別番号に対応するセンタ登録パスワード、利用者検証鍵、及び提供サービス情報が検索、抽出されると共に、サービス許可手段によって、抽出した提供サービス情報を基に、送信要求されたディジタル情報の提供の可否が判定され、この判定結果が否の場合には回線が切断され、情報センタ装置と端末装置との通信が中断される。また、判定結果が可の場合にはセッション鍵生成手段によって、セッション鍵が生成され、利用許可者指定手段によって情報を利用できる利用者が指定されると共に、署名生成手段によってディジタル署名が生成され、該ディジタル署名からセンタ署名鍵蓄積手段に蓄積されている署名鍵でセンタ署名情報が作成されて前記端末装置に送信される。

【００１０】前記センタ署名情報を受信した端末装置では、検証手段によって前記カードのセキュリティ情報蓄積手段より抽出したセンタ検証鍵を用いて、前記センタ署名情報から利用者識別番号が取り出され、照合手段により送信した利用者識別番号と比較される。この比較の結果、不一致の場合には回線が切断され、一致の場合には利用者に対して入力手段よりパスワードの入力が要求され、次いで、セッション鍵抽出手段によって前記入力されたパスワード及び前記センタ署名情報からセッション鍵が抽出される。さらに、照合手段によって前記利用者識別番号に基づいて利用者の照合が行われ、該照合結果が適合した場合に署名生成手段によって前記セッション鍵を前記カードのセキュリティ情報蓄積手段より抽出した利用者署名鍵で署名して利用者署名情報が生成され、公開鍵暗号手段で前記センタ検証鍵により前記利用者署名情報が暗号化されて前記情報センタ装置に送信される。

【００１１】前記暗号化署名情報を受信した情報センタ装置では、公開鍵復号手段で前記センタ署名鍵により前記受信した暗号化利用者署名情報が復号され、利用者署名情報が署名情報蓄積手段に蓄積される。この後、検証手段によって前記利用者署名情報から前記利用者検証鍵を用いてセッション鍵が取り出され、前記生成したセッション鍵が比較検証される。この検証の結果、一致した場合に前記送信要求されたディジタル情報がセンタ情報蓄積手段から取り出されて、慣用暗号手段によって前記セッション鍵を用いて慣用暗号化され、端末装置に送信される。

【００１２】前記暗号化ディジタル情報を受信した端末装置では、前記セッション鍵抽出手段で抽出したセッション鍵が慣用暗号手段によって前記カードのセキュリティ情報蓄積手段より抽出したグループ秘密鍵で暗号化された後、前記受信した暗号化ディジタル情報と共に、情報蓄積手段に蓄積される。

【００１３】また、情報センタ装置から受信して端末装

置内に蓄積した暗号化ディジタル情報を利用する際には、カードインタフェース手段を介して端末装置とカードが接続され、利用者に対して入力手段からのパスワードの入力が要求される。この後、前記情報蓄積手段内の利用したいディジタル情報に対応する暗号化されたセッション鍵が慣用暗号手段によって前記カードのセキュリティ情報蓄積手段より抽出したグループ秘密鍵で復号され、照合手段によって利用者の照合が行われる。この照合の結果が一致した場合に慣用暗号手段において暗号化されたセッション鍵が前記グループ秘密鍵で復号され、慣用暗号手段によって前記セッション鍵により暗号化されたディジタル情報が復号され、情報出力手段から出力される。

【００１４】これにより、システムを利用するうえで必要な利用者の情報をカードに組み込み、物理的に保護することによりカード自体の偽造等の不正行為を防止でき、さらにカードごとに異なる利用者識別番号と利用者署名鍵を組み込むことから情報の提供を受けたときの利用者を特定できる。さらに、端末装置にはセキリティ上の情報は含まれていないため、いかなる端末装置もまったく同等の条件の基に動作可能となる。

【００１５】また、請求項２記載のディジタル情報通信方法によれば、各カードごとに異なる利用者識別番号と利用者署名鍵及びグループに一つだけ共通に設定されるグループコードとグループ秘密鍵、さらにシステム共通のセンタ検証鍵を蓄積するセキュリティ情報蓄積手段を有するカードが設けられ、該カードが１グループに複数枚発行される。情報センタにディジタル情報を要求する際には、端末装置では、前記複数枚のグループカードのうちの１枚のカードから該カードの蓄積データが抽出されると共に、端末装置と情報センタ装置が接続された後、受信・蓄積する情報を利用できるグループ内の全てまたは一部のメンバーの利用者識別番号からなる利用者リストが入力手段から入力され、前記カードのセキュリティ情報蓄積手段より抽出したグループコードと利用者識別番号と共に前記利用者リストを前記情報センタ装置に送信してディジタル情報の送信が要求される。

【００１６】前記要求を受けた情報センタ装置では、利用者情報蓄積手段より前記受信した利用者識別番号に対応するセンタ登録パスワード、利用者検証鍵、及び提供サービス情報が抽出され、前記提供サービス情報を基に前記送信要求されたディジタル情報の提供の可否が判定される。該判定の結果が否の場合には回線が切断され、可の場合には疑似セッション鍵と照合セッション鍵の２種類のセッション鍵が生成され、該疑似セッション鍵と照合セッション鍵から第１の秘密関数によりセッション鍵が生成された後に、前記利用者リストに指定される利用者識別番号、前記利用者情報蓄積手段より前記グループコード及び前記指定される利用者識別番号に基づいて抽出されたセンタ登録パスワード、並びに前記照合セッション鍵から第２の秘密関数により照合用リストが作成され、前記受信した利用者識別番号並びに抽出したセンタ登録パスワード、前記疑似セッション鍵、前記照合セッション鍵及び前記照合用リストが第３の秘密関数で変換され、該変換結果をセンタ署名鍵蓄積手段より抽出したセンタ署名鍵で署名したセンタ署名情報が前記端末装置に送信される。

【００１７】前記情報を受信した端末装置では、前記センタ署名情報から前記カードのセキュリティ情報蓄積手段より抽出したセンタ検証鍵を用いて利用者識別番号が抽出れ、前記送信した利用者識別番号との検証が行なわれる。この検証の結果、不一致の場合においては端末装置と前記情報センタ装置との間の回線が切断され、一致の場合には利用者に対してパスワードの入力が要求される。この後、前記入力されたパスワード及び前記センタ署名情報を第４の秘密関数により変換して疑似セッション鍵、照合セッション鍵及び照合用リストが抽出され、前記疑似セッション鍵と前記照合セッション鍵から第１の秘密関数によりセッション鍵が構成された後、前記利用者識別番号、前記パスワード及び前記照合セッション鍵から第２の秘密関数により利用者照合データが作成される。さらに、該利用者照合データと前記照合用リストとの比較照合が行なわれ、該比較結果が不一致の場合には回線が切断され、一致の場合には前記構成したセッション鍵から前記カードのセキュリティ情報蓄積手段より抽出した利用者署名鍵を用いて利用者署名情報が生成された後、前記センタ検証鍵により前記利用者署名情報が暗号化されて前記情報センタ装置に送信される。

【００１８】前記利用者署名情報を受信した情報センタでは、前記センタ署名鍵を用いて前記暗号化された利用者署名情報が復号され、前記利用者署名情報が署名情報蓄積手段に蓄積された後、前記利用者署名情報から前記利用者情報蓄積手段に蓄積されている利用者検証鍵を用いてセッション鍵が抽出され、該抽出されたセッション鍵と前記生成したセッション鍵との照合が行われ、該照合結果が不一致の場合には回線が切断され、一致の場合には前記送信要求されたディジタル情報がセンタ情報蓄積手段から取り出され、前記ディジタル情報は前記セッション鍵で暗号化されたうえで前記端末装置に送信される。

【００１９】前記暗号化ディジタル情報を受信した端末装置では、前記セッション鍵抽出手段で抽出した疑似セッション鍵、照合セッション鍵及び照合用リストが、前記カードのセキュリティ情報蓄積手段より抽出されたグループ秘密鍵で暗号化され、前記受信した暗号化ディジタル情報と共に情報蓄積手段に蓄積される。

【００２０】また、前記情報蓄積手段に蓄積された情報を利用する際には、前記端末装置において、前記情報蓄積の際に利用したカードを含む複数枚のグループカードのうちの１枚のカードから該カードの蓄積データが抽出

されると共に、利用者に対してパスワードの入力が要求され、前記情報蓄積手段内の利用したい情報に対応する前記暗号化された照合セッション鍵及び照合用リストが前記グループ秘密鍵で復号され、前記入力されたパスワード、前記復号された照合セッション鍵及び前記カードに蓄積されている利用者蓄積番号から第２の秘密関数により利用者照合データが作成される。さらに、該利用者照合データと前記復号された照合用リストとの比較照合が行なわれ、該比較照合結果が不一致の場合には情報の利用が禁止され、一致の場合には前記暗号化された疑似セッション鍵が前記グループ秘密鍵で復号され、前記復号された疑似セッション鍵と前記照合セッション鍵から第１の秘密関数によりセッション鍵が再構成された後、前記セッション鍵により暗号化されたディジタル情報本体が復号されて情報出力手段から出力される。

【００２１】これにより、カードとパスワードが正しく入力され、かつ情報センタ装置がサービスの許可を認めないかぎり、情報の提供を受けることはできない。さらに、提供を受け、受信・蓄積した情報の利用に関しても、カードとパスワードが正しく入力され、かつ照合用リストに含まれたグループ内のメンバーだけに限定される。さらに、受信・蓄積した情報をコピーした場合には、照合用リストに含まれた人数分が最大限利用できることになるが、その場合でも利用できる人は正規のカード所有者で正しいパスワードも知っており、なおかつあらかじめ情報センタ装置が作成する照合用リストに含まれた人だけであるので、実質的に正規の利用者であると見做してよく、不正コピーとは根本的に異なるのでコピーによる著作権侵害などの問題は発生しない。

【００２２】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図１は、本発明の一実施例のディジタル情報通信システムを示す構成図である。図において、１は情報センタ装置で、端末装置との通信を制御する通信制御部１０１、後述するカード２ごとに対応するグループコードと利用者識別番号とセンタ登録パスワードと利用者検証鍵及び提供サービス情報等を蓄積する利用者情報蓄積部１０２、提供サービス情報に基づいて情報提供の可否を判定するサービス許可部１０３、セッション鍵を生成するセッション鍵生成部１０４、端末装置で受信・蓄積した情報を利用できるグループ内の全てまたは一部のメンバーを指定する利用許可者指定部１０５、センタの署名鍵を蓄積するセンタ署名鍵蓄積部１０６、ディジタル署名を生成する署名生成部１０７、公開鍵暗号方式により復号を行なう公開鍵復号部１０８、端末装置からのディジタル署名を検証する検証部１０９、端末装置からのディジタル署名を蓄積する署名情報蓄積部１１０、慣用暗号方式により暗号化を行う慣用暗号部１１１、ディジタル情報本体を蓄積するセンタ情報蓄積部１１２から構成され、これらはバスを介して互いに接続されている。

【００２３】２はグループカードとして発行されるカードで、例えば磁気カード、ＩＣカード、光記憶媒体からなるカード等を用いることが可能であり、カードごとに対応する利用者識別番号と利用者署名鍵、グループに一つだけ共通に設定されるグループコードとグループ秘密鍵、及びシステム共通のセンタ検証鍵を蓄積するセキュリティ情報蓄積部２１を備え、これらの情報内容は物理的に保護されている。

【００２４】３は端末装置で、カード２に蓄積されている情報を読み取るためのインタフェース機能を有するカード挿入部３０１、情報センタ装置との通信を制御する通信制御部３０２、情報センタからのディジタル情報を検証する検証部３０３、パスワード等を入力するためのキーボード等からなる入力部３０４、利用者の照合を行なう照合部３０５、セッション鍵を抽出するセッション鍵抽出部３０６、ディジタル署名を生成する署名生成部３０７、公開鍵暗号方式により暗号化を行なう公開鍵暗号部３０８、慣用暗号方式により暗号化／復号を行なう慣用暗号部３０９、受信情報を蓄積する情報蓄積部３１０、受信情報を読み出してディスプレー画面、音響、情報記録媒体等へ利用できる形式に出力する情報出力部３１１から構成され、これらはバスを介して互いに接続されている。

【００２５】次に、前述の構成よりなる本実施例において端末装置３が情報センタ装置１から情報を受信し、蓄積するまでの動作手順（情報配送過程）を図２に示すフローチャートに基づいて説明する。

【００２６】まず、情報センタ装置１内の情報を端末装置３に受信・蓄積したい利用者は、自分のカード２を端末装置３のカード挿入部３０１に挿入する。次いで、通信制御部３０２，１０１を介して情報センタ装置１に接続した後、今回受信・蓄積する情報を利用できるグループ内のメンバーを任意に指定し、指定したメンバーの利用者識別番号ＡＩＤｊの集合からなる利用者リストＬＩＤを入力部３０４から入力し、前記利用者リストＬＩＤと前記カード２のセキュリティ情報蓄積部２１から抽出したグループコードＧＣと利用者識別番号ＵＩＤｊとを合わせて情報センタ装置１に送信し、ディジタル情報Ｍの送信を要求する（ＳＡ１）。尚、カード２のセキュリティ情報蓄積部２１には図３に示すように、グループコードＧＣ、利用者識別番号ＵＩＤｉ、センタ検証鍵Ｃｐ、利用者署名鍵Ｄｉ、グループ秘密鍵ＧＫの情報が含まれており、これらの情報内容は物理的に保護されている。

【００２７】情報センタ装置１では、図４に示すフォーマット形式でグループコードＧＣｄ、利用者識別番号ＵＩＤｎ、センタ登録パスワードＰＷｎ、利用者検証鍵Ｅｎ、及び提供サービス情報が蓄積されている利用者情報蓄積部１０２より、端末装置３から受信した利用者識別番号ＵＩＤｉに対応するセンタ登録パスワードＰＷｉ、

利用者検証鍵Ｅｉ、及び提供サービス情報ＳＶｉを検索、抽出する（ＳＡ２）。

【００２８】次いで、サービス許可部１０３において抽出した提供サービス情報ＳＶｉを基に、送信要求されたディジタル情報の提供の可否を判定し（ＳＡ３）、この判定結果が否の場合には回線を切断し（ＳＡ４）、情報センタ装置１と端末装置３との通信を中断する。また、判定結果が可の場合にはセッション鍵生成部１０４において、疑似セッション鍵ＫＳＩと照合セッション鍵ＫＳ２の２種類のセッション鍵を生成し、さらに疑似セッション鍵ＫＳ１と照合セッション鍵ＫＳ２から第１の秘密関数ｆ１（）により情報本体の暗号化用セッション鍵ＫＳを生成する（ＳＡ５）。尚、疑似セッション鍵ＫＳ１及び照合セッション鍵ＫＳ２の生成方法としては、例えば６４ビットの乱数列を使用することができる。また、第一の秘密関数ｆ１()には例えば、次の(1) 式を用いることができる。

【００２９】

【数１】

$$f1(KS1, KS2) = KS1(rot16) \oplus KS2 = KS \quad \cdots(1)$$

ただし、ＫＳ１（ｒｏｔ１６）はＫＳ１の左１６ビットシフトを、
⊕は排他的論理和を表す。

この後、利用許可者指定部１０５において照合セッション鍵ＫＳ２、利用者リストＬＩＤに含まれる各利用者ごとの利用者識別番号ＡＩＤｊ、及びグループコードＧＣと各利用者ごとの利用者識別番号ＡＩＤｊに基づいて前記利用者情報蓄積部１０２より抽出されたセンタ登録パスワードＡＰＷｊとから第２の秘密関数ｆ２（）により照合用個人リストＡＬＴｊを作成すると共に、前記照合用個人リストＡＬＴｊの集合からなる照合用リストＡＬＴを作成する（ＳＡ６）。

【００３０】図５に前記利用者リストＬＩＤと照合用リストＡＬＴのデータ形式を示す。尚、グループコードが異なる利用者識別番号が含まれている場合には、該利用者識別番号についてのみ無効とする。また、第２の秘密関数ｆ２（）には例えば、次の(2) 式を用いることができる。

【００３１】

【数２】

$$f2(KS2, AIDi, APWj) = h(KS2 \,||\, AIDj \,||\, APWj) = ALTj \quad \cdots(2)$$

ただし、ｈ（）はハッシュ関数を、||はビット連結を表す。

最後に、署名生成部１０７において前記受信した利用者識別番号ＵＩＤｉ並びに抽出した前記センタ登録パスワードＰＷｉ、疑似セッション鍵ＫＳ１、照合セッション鍵ＫＳ２及び照合用リストＡＬＴを第３の秘密関数ｆ３（）により変換した後、該変換結果からセンタ署名鍵蓄積部１０６に蓄積されている署名鍵Ｃｓでセンタ署名情報ＣＳｉｇｎを作成し（ＳＡ７）、前記端末装置２に送信する。尚、第３の秘密関数ｆ３（）には例えば、次の(3) 式を用いることができる。

【００３２】

【数３】

$$CSign = Cs(F3(UIDi, PWi, KS1, KS2, ALT)) = F3(UIDi, PWi, KS1, KS2, ALT) \,||\, PWi \oplus KS1 \text{ 以 } PWi \oplus KS2 \text{ を抽出した後} \quad \cdots(3)$$

【００３３】次いで、端末装置３では、次の(4) 式に示すように、検証部３０３において前記カード２のセキュリティ情報蓄積部２１より抽出したセンタ検証鍵Ｃｐを用いて、前記センタ署名情報ＣＳｉｇｎから利用者識別番号を取り出し、送信した利用者識別番号ＵＩＤｉと比較する（ＳＡ８）。

【００３４】

【数４】

$$Cp(CSign) = Cp(Cs(f3(UIDi, PWi, KS1, KS2, ALT))) = f3(UIDi, PWi, KS1, KS2, ALT) \quad \cdots(4)$$

この検証の結果、不一致の場合には回線を切断し（ＳＡ９）、一致の場合には利用者に対して入力部３０４よりパスワードＰＷｉの入力を要求し、次いで、セッション鍵抽出部３０６において前記入力されたパスワードＰＷｉ及び前記センタ署名情報ＣＳｉｇｎから第３の秘密関数ｆ３（）の逆変換（第４の秘密関数）により疑似セッション鍵ＫＳ１、照合セッション鍵ＫＳ２，及び照合用セッション鍵ＫＳ１と照合セッション鍵ＫＳ２から第１の秘密関数ｆ１（）によりセッション鍵ＫＳを構成する（ＳＡ１０）。

【００３５】次に、照合部３０５において前記利用者識別番号ＵＩＤｉ、パスワードＰＷｉ及び照合セッション鍵ＫＳ２から第２の秘密関数ｆ２（）により利用者照合データを作成し（ＳＡ１１）、該利用者照合データと前記照合用リストＡＬＴに含まれる照合用個人リストＡＬＴｊ全てとの比較照合を行ない（ＳＡ１２）、全て不一致の場合には回線を切断し（ＳＡ１３）、一致するものがある場合には署名生成部３０７において前記セッション鍵ＫＳを前記カード２のセキュリティ情報蓄積部２１より抽出した利用者署名鍵Ｄｉで署名して利用者署名情報Ｓｉｇｎ［Ｄｉ（ＫＳ）］を生成し（ＳＡ１４）、公開鍵暗号部３０８で前記センタ検証鍵Ｃｐにより前記利用者署名情報を暗号化して（ＳＡ１５）前記情報センタ装置１に送信する。

【００３６】前記情報センタ装置１では、公開鍵復号部１０８で前記センタ署名鍵Ｃｓにより前記受信した暗号

化利用者署名情報を復号し（ＳＡ１６）、利用者署名情報Ｓｉｇｎを署名情報蓄積部１１０に蓄積する（ＳＡ１７）。この後、検証部１０９において前記利用者署名情報Ｓｉｇｎから前記利用者検証鍵Ｅｉを用いてセッション鍵を取り出し、前記生成したセッション鍵ＫＳを比較検証する（ＳＡ１８）。この検証の結果、不一致の場合には回線を切断し（ＳＡ１９）、一致の場合には前記送信要求されたディジタル情報Ｍをセンタ情報蓄積部１１２から取り出して、慣用暗号部１１１において前記セッション鍵ＫＳにより慣用暗号化［ＫＳ（Ｍ）］をしたうえで（ＳＡ２０）端末装置３に送信する。

【００３７】前記端末装置３では、前記セッション鍵抽出部３０６で抽出した疑似セッション鍵ＫＳ１、照合セッション鍵ＫＳ２及び照合用リストＡＬＴを慣用暗号化部３０９において前記カード２のセキュリティ情報蓄積部２１より抽出したグループ秘密鍵ＧＫで暗号化した後（ＳＡ２１）、前記受信した暗号化ディジタル情報と共に、図６に示すフォーマット形式に従って情報蓄積部３１０に蓄積する（ＳＡ２２）。

【００３８】次に、情報センタ装置１から受信して端末装置３内に蓄積したディジタル情報を利用する場合の動作手順（情報利用過程）を図７のフローチャートに基づいて説明する。蓄積した情報を利用する際には、端末装置３において、カード挿入部３０１にカード２を挿入した後、利用者に対して入力部３０４からパスワードＰＷｉの入力を要求する（ＳＢ１）。

【００３９】次に、情報蓄積部３１０内の利用したいディジタル情報に対応する暗号化された照合セッション鍵ＧＫ（ＫＳ２）及び照合用リストＧＨ（ＡＬＴ）を慣用暗号部３０９において前記カード２のセキュリティ情報蓄積部２１より抽出したグループ秘密鍵ＧＫで復号化し（ＳＢ２）、照合部３０５において前記パスワードＰＷｉ、照合セッション鍵ＫＳ２及びカード２のセキュリティ情報蓄積部２１より抽出した利用者識別番号ＵＩＤｉから第２の秘密関数ｆ２（）により利用者照合データを作成して（ＳＢ３）、該利用者照合データと前記照合用リストＡＬＴに含まれる照合用個人リストＡＬＴｊ全てとの比較照合を行なう（ＳＢ４）。

【００４０】この照合の結果、全て不一致の場合には情報の利用を禁止し（ＳＢ５）、一致するものがある場合には慣用暗号部３０９において暗号化された疑似セッション鍵ＧＫ（ＫＳ１）を前記グループ秘密鍵ＧＫで復号化し（ＳＢ６）、前記照合セッション鍵ＫＳ２と共に第１の秘密関数ｆ１（）によりセッション鍵ＫＳを再構成した後（ＳＢ７）、慣用暗号部３０９において前記セッション鍵ＫＳにより暗号化されたディジタル情報ＫＳ（Ｍ）を復号し（ＳＢ８）、情報出力部３１１から出力する（ＳＢ９）。

【００４１】以上説明したように、情報センタ装置１から受信して端末装置３に蓄積した情報は、照合用リストに記載されている利用者が正しいカード２と正しいパスワードＰＷｉを使用したときのみに利用することが可能である。従って、情報をコピーされても不正に利用される心配はないので、コピー禁止等の制限を付ける必要はない。

【００４２】また、情報を利用するのに必要な鍵である照合用リスト、照合セッション鍵、疑似セッション鍵、セッション鍵はそれぞれ関連し合って使用されているので、利用を許可されていない別の情報について一部または全部を改竄して不正に利用しようとしても、改竄の影響が情報を利用するのに必要な鍵すべてに広がるので情報を不正に利用できる状態にはならない。これらのことから、情報の著作権保護が保証される。

【００４３】一方、このシステムは家族や会社内のセクション、同好会など閉じたグループを対象とし、情報のアクセス権限機能を含んだディジタル情報通信システムでもある。即ち、グループのメンバーには各自のパスワードと利用できるサービスの種類を規定した提供サービス情報の登録と引き替えに、各自に対して一枚づつグループカード２が情報提供業者から渡され、そのカード２にはグループ共通のグループコードとグループ秘密鍵、システム共通のセンタ検証鍵、カード２ごとに異なる利用者識別番号と利用者署名鍵が記録されている。このため、情報の提供を受ける場合には利用者署名鍵が使われるので、グループのメンバーが複数いても誰が情報の提供を受けたのかが特定できる。

【００４４】また、照合用リストはグループコードと情報を利用できるメンバーを指定した利用者リストを基に、一人づつ情報センタ装置（情報提供業者）が自動的にパスワードを組み込んで作成されるので、メンバーのパスワードを知る必要はないうえ、別グループの人が照合用リストに組み込まれることもない。

【００４５】さらに、情報の利用に関しては、その情報の照合用リストに含まれていないメンバーでは利用者識別番号とパスワードの組み込みが行なわれていないため、たとえ同じグループのメンバーであっても利用することはできない。一方、照合用リストに含まれているメンバーは自由に利用することが可能であり、必要ならば情報をコピーして利用しても構わない。つまり、コピーして利用できるのは照合用リストに記載されているメンバーだけであり、情報提供業者が照合用リストを自ら作成するので、照合用リストの人数によって情報料金を変更するなどにより、照合用リストに含まれているメンバーをすべて正規のユーザであると見做すことができるからである。

【００４６】

【発明の効果】以上説明したように本発明の請求項１記載のディジタル情報通信システムによれば、システムを利用するうえで必要な利用者の情報をカードに組み込み、その情報に関しては物理的に保護されたカードと、

カードを挿入し、正しいパスワードを入力することにより使用可能となる端末装置、及びセッション鍵を設定し、そのセッション鍵でディジタル情報を暗号化した後に端末装置へ送信する情報センタ装置を具備しているので、カード自体の偽造等の不正行為を防止でき、さらにカードごとに異なる利用者識別番号と利用者署名鍵を組み込むことから情報の提供を受けたときの利用者を特定することができる。また、端末装置にはセキュリティ上の情報は含まれていないため、いかなる端末装置もまったく同等の条件の基に動作させることができる。

【００４７】また、請求項２記載のディジタル情報通信方法によれば、グループカードとして複数人で構成される１グループに人数分の枚数のカードを提供し、各々のカードについて情報センタ装置から提供を受けることのできるディジタル情報のサービスを規定し、さらに情報センタ装置から提供を受けて端末装置に受信・蓄積したディジタル情報について、グループ内でも利用できるメンバーを特定することができるので、カードとパスワードが正しく入力され、かつ情報センタ装置がサービスの許可を認めないかぎり、情報の提供を受けることはできない。また、提供を受け、受信・蓄積した情報の利用に関しても、カードとパスワードが正しく入力され、かつ照合用リストに含まれたグループ内のメンバーだけに限定される。さらに、受信・蓄積した情報をコピーした場合には照合用リストに含まれた人数分が最大利用できることになるが、その場合でも利用できる人は正規のカード所有者で正しいパスワードも知っており、なおかつあらかじめ情報センタ装置が作成する照合用リストに含まれた人だけであるので、実質的に正規の利用者であると見做せ、不正コピーとは根本的に異なるのでコピーによる著作権侵害などの問題は発生しない。

【図面の簡単な説明】

【図１】本発明の一実施例のディジタル情報通信システムを示す構成図

【図２】一実施例におけるディジタル情報通信方法での情報配送過程における動作手順を示すフローチャート

【図３】一実施例におけるカード内のセキュリティ情報蓄積部に蓄積されている情報内容を示す図

【図４】一実施例における情報センタ装置内の利用者情報蓄積部に蓄積されているデータ形式の説明図

【図５】一実施例における利用者リストと照合用リストのデータ形式の説明図

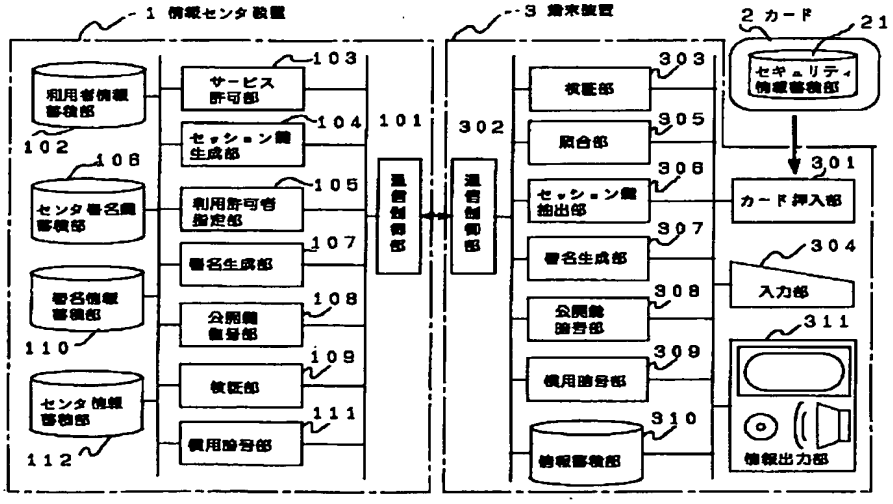
【図６】一実施例における端末装置内の情報蓄積部に蓄積するときのデータ形式の説明図

【図７】一実施例におけるディジタル情報通信方法での情報利用過程における動作手順を示すフローチャート

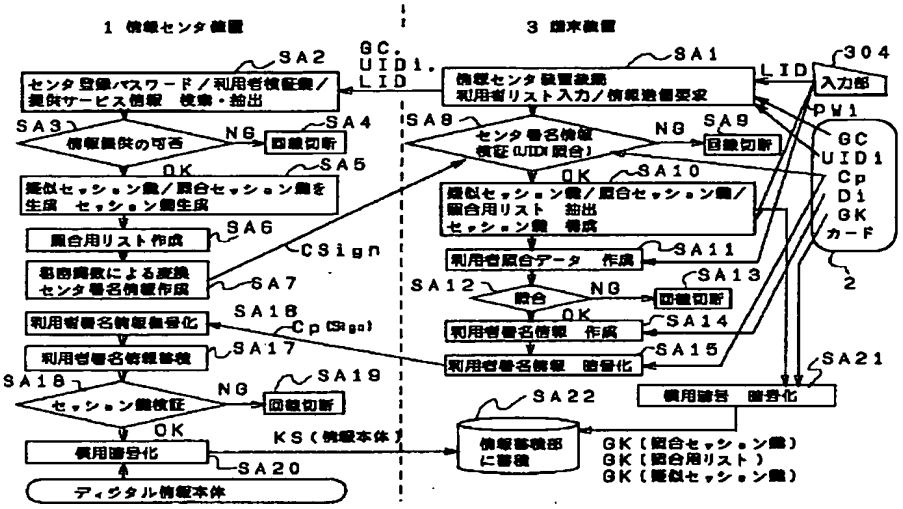
【符号の説明】

１…情報センタ装置、１０１…通信制御部、１０２…利用者情報蓄積部、１０３…サービス許可部、１０４…セッション鍵生成部、１０５…利用許可者指定部、１０６…センタ署名鍵蓄積部、１０７…署名生成部、１０８…公開鍵復号部、１０９…検証部、１１０…署名情報蓄積部、１１１…慣用暗号部、１１２…センタ情報蓄積部、２…グループカード、２１…セキュリティ情報蓄積部、３…端末装置、３０１…カード挿入部、３０２…検証部、３０３…検証部、３０４…入力部、３０５…照合部、３０６…セッション鍵抽出部、３０７…署名生成部、３０８…公開鍵暗号部、３０９…慣用暗号部、３１０…情報蓄積部、３１１…情報出力部。

【図１】



【図２】



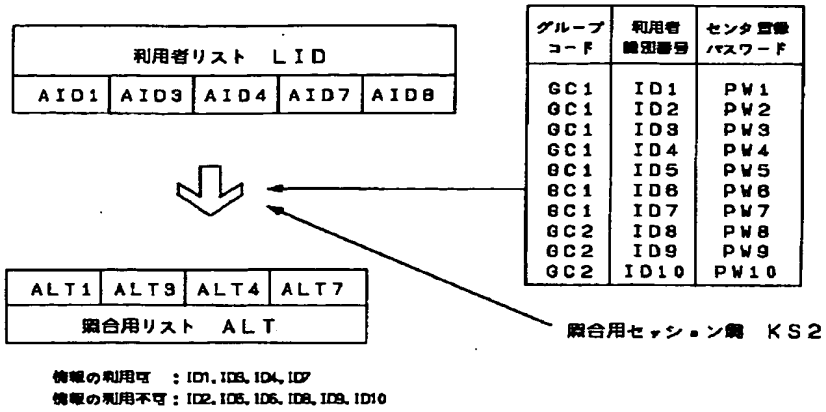
【図３】

グループコード GC	利用者識別番号 UIDi	センタ検証鍵 Cp	利用者署名鍵 Di	グループ秘密鍵 GK

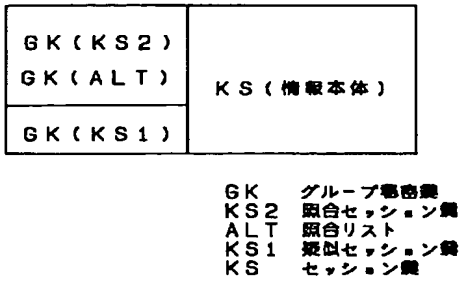
【図４】

グループコード	利用者識別番号	センタ登録パスワード	利用者検証鍵	提供サービス情報			
				情報１	情報２	・・・・	情報ｋ
GC1	UID1	PW1	E1	○	○	・・・・	○
GC1	UID2	PW2	E2	○	×	・・・・	×
：	：	：	：	：	：	・・・・	：
：	：	：	：	：	：	・・・・	：
GCd	UIDn	PWn	En	○	○	・・・・	×
：	：	：	：	：	：	・・・・	：

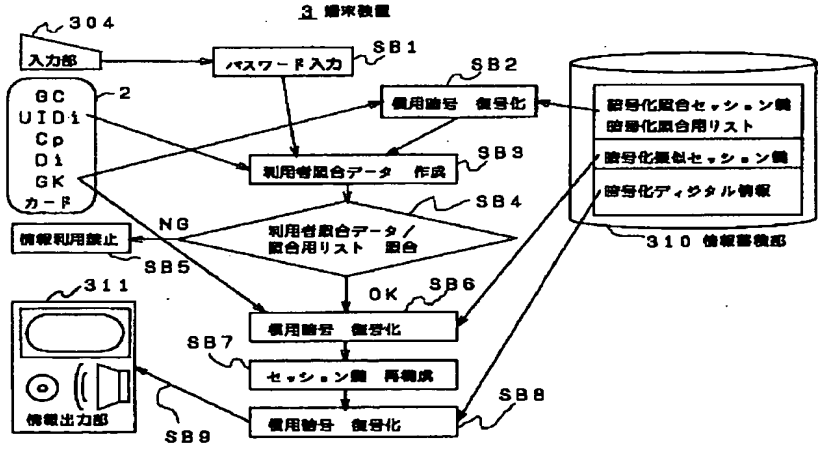
【図５】



【図６】



【図７】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		9364－5Ｌ		